UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/766,869	01/30/2004	Katsuyuki Umezawa	62807-159	4096

7590 06/19/2007

McDermott, Will & Emery
600, 13th Street, N.W.
Washington, DC 20005-3096

EXAMINER	
PALIWAL, YOGESH	
ART UNIT	PAPER NUMBER
2135	
MAIL DATE	DELIVERY MODE
06/19/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/766,869	UMEZAWA ET AL.	
	Examiner	Art Unit	
	Yogesh Paliwal	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-9 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-9 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 30 January 2004 is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date 1/30/2004.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Priority

1. Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Specification

2. The disclosure is objected to because of the following informalities:

On page 14 line 28, "first service provider" should read, "~~first~~ second service provider".

Appropriate correction is required.

Claim Objections

3. Claims 1-9 are objected to because of the following informalities:

- Claim 1 line 25 (Page 24), please replace "said" with "a" [Note: this certificate is a certificate of the CA, which is not generated previously in claim 1, as a result it lacks antecedent basis].
- Claim 1 line 31 (Page 25) should read, "said smart card <u>further</u> comprises a certificate".

<u>Claims 2-9 are also objected for being dependent on claim 1.</u>

- Claim 2 line 2 (Page 25) should read, "said certificate authority <u>further</u> comprises".

- Claim 2 lines 4 and 5 (Page 25), both lines include phrase "the certificate", however it is not clear as to which certificate this claim limitation is referring to because claim 1 produces 3 different certificates.

Claims 7-9 are also objected for being dependent on claim 2.

- Claim 4 line 2 recites a limitation "said service provider specific area", which lacks antecedent basis. Currently claim 4 depends on claim 1 and claim 1 does not provide antecedent basis for the limitation "said service provider specific area", however, claim 3 provides antecedent basis for this claim limitation. As a result examiner suggest claim 4 should depend on claim 3 and not on claim 1. For the purposes of examination claim 4 will be assumed to depend from claim 3.
- Claim 5 line 5 (Page 25), recites limitation "the certificate", however it is not clear as to which certificate this claim limitation is referring to because claim 1 produces 3 different certificates.
- Claim 5 lines 5-6 (Page 25), recite limitation "said certificate verifying unit", which lacks antecedent basis. Please replace "said" with "a".
- Claim 6 line 7 (Page 26), Please replace "certificate" with "certificates".
- Claim 7 line 11 (Page 27) should read, "said service provider further comprises".

Claims 8-9 are also objected for being dependent on claim 7.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1,2,4,5,7,8 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Hamann et al. (US 2002/0026578 A1), hereinafter Hamann, with Dare et al. (US 2003/0163687 A1), hereinafter Dare.

Regarding **Claim 1**, Hamann discloses a management system of a public key certificate comprising:

a service provider which verifies validity of a presented public key certificate and, if the verification can correctly be made, provides a service **(Paragraph 0046, lines 6-10, here, application is referred as a software module running in the service provider's server, which verifies the standard information of the digital certificate)**

a certificate authority on which said service provider relies **(Paragraph 0031, line 3, CA)**; and

a smart card **(Fig.1)**,

wherein said smart card comprises:

a storing unit **(Fig. 1, EPROM)** which stores

a first private key and a first public key making a pair together therewith which are necessary to issue a certificate to said certificate authority **(Fig. 2, Numeral 8, user's Public Key 1, Users Private Kay 1)**,

a first certificate issued for said first public key **(Fig. 2, numeral 6, User's certificate # 1)**,

a second private key and a second public key making a pair together therewith which are generated to receive a service from said service provider **(Fig. 2, numeral n, when n =2,)**, and

a second certificate which is issued for said second public key by said certificate authority on which said service provider relies **(Fig. 2, User's certificate when n =2);** and

a key generating unit which generates said first and second public keys and said first and second private keys **(Paragraph 0025, "A cryptographically processor"),**

said certificate authority comprises:

a storing unit which stores a third private key for generating a certificate of said second public key for said smart card **(Paragraph 0031, line 7-8, "the CA generates a new user certificate for a new public key". Reference doesn't explicitly teaches that CA stores it's own public and private key, however, it is an inherited feature of CA that it always have storage unit which store it's own private key and a corresponding public key, from which the private key is used to generate user certificates)** and

a certificate generating unit which generates the second certificate for said second public key on the basis of an issuing request **(Paragraph 0031, "...the CA generates a new user certificate for a new public key")**, and

Hamann does not explicitly teaches a certificate which is issued to a third public key making a pair together with said third private key [certification of a CA who is providing the certificate to the user]. Hamann also does not teach that the smart card further comprises a certificate generating unit which issues the certificate of said certificate authority by using said stored first private key on the basis of an issuing request for the certificate from said certificate authority.

However, Dare, in the same field of endeavor of digital certificate management, discloses a certificate issued to CA for CA's public key using root CA's private key **(Fig. 2B, numerals 228 and 229, also at paragraph 0064, "The authentication block 228 is signed using the private key of the bank 222")**

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to have a CA of Hamann reference to certify it's public key with other CA that the user of smart card trust as suggested by Dare reference *so that user of smart card can trust the CA which is going to certify public key of the user of the smart card.*

Further Dare discloses smart card **(Paragraph 0016, "Password-protected smart card")** comprising certificate generating unit which issues the certificate of certificate authority by using said stored first private key on the basis of an issuing request for the certificate from said certificate authority **(Paragraph 0026, "...each**

node having a private and public key pair, the nodes being either or both a certifying node and a certified node, a certifying node providing a digital certificate making reference to the public key of a certified node and the digital certificate being signed by the private key of the certifying node").

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to let the smart card of Hamann generate the certificate of CA by using private key as suggested by Dare to *"enable a user [smart card] to choose a root from which to obtain a root public key from any node in a PKI and to enable the user to use the root public key as a global root key to obtain a chain of certificates along a path to any other node in the PKI"* ***(Dare, Paragraph 0025)***

Regarding **claim 2**, the rejection of claim 1 is incorporated and further Hamann discloses that said smart card presents said first and second certificates to said service provider in order to receive the service from said service provider **(Paragraph 0046, lines 6-10)**, and

said service provider comprises:

a certificate verifying unit for inquiring of said certificate authority about the revocation information of said first and second certificates when the validity of said presented first and second certificates is verified **(Paragraph 0046, lines 6-12)**

Hamann reference does not explicitly teach that certificate authority further comprises:

a revocation information generating unit for generating revocation information of the certificate on the basis of a revoking request for the certificate; and a revocation

information database for storing the revocation information generated by said revocation information generating unit, however, these limitations are generally associated with certificate authority and Dare reference in the background section provides support for this statement. Dare discloses:

a revocation information generating unit for generating revocation information of the certificate on the basis of a revoking request for the certificate **(Paragraph 0020, lines 1-4)** ; and

a revocation information database for storing the revocation information generated by said revocation information generating unit **(Paragraph 0020, lines 4-7)**.

Regarding **Claim 4**, the rejection of claim 3 [Claim 4 is assumed to be dependent from claim 3, as described above) is incorporated and further Hamann and Dare combination discloses wherein said service provider specific area of said smart card and data stored in said certificate generating unit have been encrypted **(Dare, Paragraph 0016, "For public key encryption to be effective, a user must keep his private key secret. For example, this could be done by a password-protected smart card").**

Regarding **Claim 5**, the rejection of claim 1 is incorporated and further Dare discloses that system further comprising a certificate validation authority, and

said certificate validation authority making validity verification of the certificate by said certificate verifying unit of said service provider as an alternative of said service provider **(Paragraph 0019, RA can provide validation)**

Regarding **Claim 7**, the rejection of claim 2 is incorporated and further the combination of Hamann and Dare discloses wherein when said certificate authority verifies said second certificate, said service provider transmits a challenge to said smart card **(Dare, Paragraph 0092, line 4-5, "Accordingly, a random challenge is sent by the user [service provider] to the sender [smart card with the certificate]")**,

said smart card encrypts said challenge by said second private key and transmits said encrypted challenge, the second certificate corresponding to said second private key, and the first certificate corresponding to said first private key to said service provider **(Dare, Paragraph 0092, "he [smart card] encrypts it with his private key")**,

said service provider further comprises:

a certificate verifying unit for decrypting said encrypted challenge **(Dare, Paragraph 0092, "the user decrypts it with the public key from the certificate")**, confirming whether the decrypted challenge coincides with said challenge transmitted to said smart card **(Paragraph 0092, "If that gets the user back to the original challenge, then the sender has been authenticated as the certificate holder")** , obtaining the revocation information of said received first and second certificates, and executing the verifying process of said first and second certificates by using said obtained revocation information **(Paragraph 0088, paragraph 0089 and paragraph 0090, first certificate is scheme's certificate and second certificate is member**

certificate. It can be seen that verifier verifies that neither the scheme certificate nor the member certificate has been revoked"); and

a service providing unit for providing the services in response to a decision indicating that said first and second certificates are valid in said verifying process **(Hamann, Paragraph 0017, "Any application using the user certificates and its related user private keys on the token is able to verify the user certificate [in this case both certificates as taught by the combination of Hamann and Dare]", Hamann doesn't explicitly teaches that after the authentication the application provides service to the user of smart card, however, it is generally the case that user of smart card get some sort of service from the application requiring the certificate authentication]**

Regarding **claim 8**, the rejection of claim 7 is incorporated and further Hamann discloses said smart card constructs said storing unit as an area specific to said service provider **(Fig. 2, It is clear from the figure that different application [service providers] save their corresponding key pairs and certificates in area specified to that application as illustrated by Fig. 2)** and,

when said service provider transmits and receives data to/from said service provider specific area, said service provider executes a mutual authenticating process between said service provider and said service provider specific area **(Paragraph 0046, lines 1-9).**

Regarding **Claim 9**, the rejection of claim 7 is incorporated and further combination of Hamann and Dare discloses that when data is stored into said service provider specific area of said smart card and into said certificate generating unit, said data is encrypted and thereafter stored **(Dare, Paragraph 0016, "For public key encryption to be effective, a user must keep his private key secret. For example, this could be done by a password-protected smart card").**

Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Hamann et al. (US 2002/0026578 A1), hereinafter Hamann, with Dare et al. (US 2003/0163687 A1), hereinafter Dare and further in view of Audebert et al. (US 2003/0005317 A1), hereinafter Audebert.

Regarding **Claim 3,** the rejection of claim 1 is incorporated and further Hamann discloses wherein said smart card construct said storing unit as an area which is specific to said service provider **(Fig. 2, It is clear from the figure that different application [service providers] save their corresponding key pairs and certificates in area specified to that application as illustrated by Fig. 2)**

Hamann does not disclose a service provider authenticating unit for permitting only said service provider corresponding to said specific area to access said specific area.

However, Audebert, discloses a service provider authenticating unit for permitting only service provider corresponding to specific area to access specific area **(Paragraph 0012, "Each domain allow access to common utilities and services installed in the**

PSD [PSD stands for personal security devices that includes smart card, as established by Audebert in paragraph 0002] but the PSD's security policies prevent accessing of secure information installed outside of a providers allocated domain").

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to permit access of service providers of Hamann to only access the area that is specific to that service provider as taught by Audebert so that *"multiple sets of separately accessible keys may exist within a PSD at any one time but only the owner of the keys may access the domain in which they are installed"* **(Audebert, Paragraph 0012).**

Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Hamann et al. (US 2002/0026578 A1), hereinafter Hamann, with Dare et al. (US 2003/0163687 A1), hereinafter Dare and further in view of Doyle et al. (US 6,438,550 B1), hereinafter Doyle.

Regarding **Claim 6**, the rejection of claim 1 is incorporate and the combination of Hamann and Dare does not disclose a certificate storage authority, and said certificate storage authority holding a plurality of certificates stored in said smart card as an alternative of said smart card and providing said certificate in accordance with a request.

However, Doyle et al. (US 6,438,550 B1), hereinafter Doyle, discloses certificate storage authority holding a plurality of certificates stored in smart card as an alternative

of smart card and providing certificate in accordance with a request **(Column 5, lines 60-64, "Alternatively, certificate 408 and private key 410 may be stored on some other type of storage device, such as, for example, a floppy disk, a hard drive, or a CD-ROM encrypted by a PIN")**

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to store certificates of smart card of Hamann in an external storage unit as an alternative as suggested by Doyle because "the size of an end user's public key Infrastructure (PKI) key-ring often will exceed the storage capacity of even the largest smart card" **(Doyle, Column 1, lines 45-47).**

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yogesh Paliwal whose telephone number is (571) 270-1807. The examiner can normally be reached on M-F: 7:30 AM - 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

YP
AU 2135
5/30/07

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100